
Article:
Roberts, George L., Lucamarini, Marco orcid.org/0000-0002-7351-4622, Dynes, James F. et al. (3 more authors) (2017) Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution. Applied Physics Letters. 261106. ISSN 0003-6951

https://doi.org/10.1063/1.5004488

Applied Physics Letters

Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution

Cite as: Appl. Phys. Lett. **111**, 261106 (2017); https://doi.org/10.1063/1.5004488
Submitted: 13 September 2017 . Accepted: 12 December 2017 . Published Online: 27 December 2017

George L. Roberts, Marco Lucamarini, James F. Dynes, Seb J. Savory, Zhiliang Yuan, and Andrew J. Shields

Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution

George L. Roberts,[1,2,a)] Marco Lucamarini,[1] James F. Dynes,[1] Seb J. Savory,[2] Zhiliang Yuan,[1] and Andrew J. Shields[1]
[1]*Toshiba Research Europe Ltd, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom*
[2]*Cambridge University Engineering Department, 9 J J Thomson Avenue, Cambridge CB3 0FA, United Kingdom*

(Received 13 September 2017; accepted 12 December 2017; published online 27 December 2017)

Distributed-phase-reference (DPR) systems were introduced as a method of decreasing the complexity of quantum key distribution systems for practical use. However, their information-theoretic security has only been proven when the added requirement of block-wise phase randomisation is met. Realisation of this with a conventional approach would result in a cumbersome transmitter, removing any practical advantage held by DPR systems. Here, we solve this problem using a light source that allows the coherence between pulses to be controlled on a pulse-by-pulse basis without the need for additional bulky components. The system is modulator-free, does not require a complex receiver, and features an excellent stability without an active stabilisation mechanism. We achieve megabit per second key rates that are almost three times higher than those obtained with the standard Bennet-Brassard 1984 protocol. https://doi.org/10.1063/1.5004488

Quantum key distribution (QKD) has developed strongly since the proposal of the first protocol in 1984.[1–3] The future could see widespread quantum networks similar to those in Tokyo[4] and Vienna[5] and global secure communication enabled by QKD over satellites.[6] These advances depend on the development of simple, cost-effective, and high performance implementations. Innovations in both protocols and system hardware are required to achieve this.

Nearly two decades after the inception of Bennett-Brassard 1984 (BB84),[1] distributed phase reference (DPR) QKD was proposed, allowing for much simpler experimental implementations. The class includes the differential phase shift,[7,8] coherent-one-way,[9,10] and differential phase time shift[11] protocols. One advantage is that the transmitters needed to realize these DPR protocols can be made using off-the-shelf telecom lasers and modulators. However, the benefit of their simpler implementation is outweighed by a seriously degraded performance when full security is taken into account.[3,12,13] This is because the pulse pairs in BB84 are phase randomized, making it possible to decompose the general multi-pulse state into independent signals, which can be analysed with current security proofs. Photons in DPR protocols, on the contrary, are coherently spread across many pulses, making the security analysis more cumbersome. To plug the security gap, two further DPR protocols were proposed: round-robin differential phase shift and differential quadrature phase shift (DQPS). The former simplifies the estimation of Eve's information but requires an overly complicated QKD receiver setup,[14–17] making it impractical. The latter separates the signal from the differential phase shift protocol into blocks, each having a global phase that varies randomly, ensuring that the protocol is immune against coherent attacks.[18,19] It does, however, stray from the main goal of DPR protocols to provide simpler QKD implementations, due to the phase randomization requirement, which prohibits a low complexity implementation of the protocol using current transmitter systems.

In this work, we show that it is possible to produce phase coherent and phase randomized pulses from a single device. This device is based on the optical injection of one laser diode (LD) into another, removing the need for a phase-randomization component in DQPS by relying on the randomness provided by spontaneous emission.[20] This transmitter is stable, has a small footprint, and allows us to achieve a base quantum bit error rate (QBER) of just 2.15%. We obtain a secure key rate of 2.37 Mbit/s at short distances and show positive key rates up to an equivalent distance of 110 km. The secure key rates measured using real optical fiber channels align well with those obtained using an optical attenuator. We also compare the secure key rates obtained with both protocols and find that, on average, DQPS produces keys at a rate 2.71 higher than the commonly adopted BB84 protocol. Finally, we show that the lack of an interferometer in the transmitter enables a stability over three days with no active feedback. This kind of free-running stability has not been seen before and would enable far more simplicity in future QKD implementations. It also increases the sifted key rate because no stabilisation pulses are required.

The differential phase shift protocol was the first DPR protocol proposed. In this system, Alice encodes one of the two random orthogonal phase values onto a coherent stream of pulses. Bob then measures the bit values using an interferometer, inferring the presence of Eve by a break in coherence of the pulses during communication.

a)Electronic mail: glr28@cam.ac.uk

The DQPS protocol splits the differential phase shift signal into blocks of length L. Each of these blocks has a globally random phase, which removes the coherence between pulses in different blocks. Four phases are used in two non-orthogonal bases. These act as the data Z $\{0, \pi\}$ and check X $\{\pi/2, 3\pi/2\}$ bases. We note that with a block size $L = 2$, the DQPS protocol is identical to the phase-encoded BB84 protocol.

For implementation, the protocol starts with Alice randomly deciding her encoding basis for each block and bit value for each pulse inside the block. She gives each block a globally random phase before sending them to Bob. Bob uses a Mach-Zehnder interferometer (MZI) with a one-bit time delay to measure the phase of each pulse in a randomly determined basis for each block. If Bob detects a photon in a block, he discards any other photon clicks that occur at a later time in the same block. If both detectors click at the same time, he randomly assigns a measurement. Bob announces when he measured a pulse in each block, allowing Alice to determine a raw key. They then announce which basis they used for each pulse, allowing them to share a sifted key and then perform error correction and privacy amplification.

A security proof is outlined by Kawakami *et al.*[19] that draws on a modified tagging technique and the complementarity argument.[21] The ordinary tagging technique for phase-encoded BB84 marks a pulse-pair at Alice as completely insecure if it contains more than one photon. Alice can in principle perform a projective measurement of the total photon number in a pair, allowing her to discard these pulses. In the DQPS protocol, however, a pulse pair is defined only after Bob performs his measurement. At that point, it is too late for Alice to perform her photon measurement. The modified proof assumes that Alice stores auxiliary qubits to perform a photon number measurement when she knows Bob's measurement time. Hence, it becomes possible to statistically determine r_{tag} as the probability of a single block having two or more photons distributed in a single pulse or in two adjacent pulses.

Using this, the extracted asymptotic key rate is given by

$$R = \frac{n_{\text{rep}} p_0^2 Q}{L}\left[1 - f_{\text{PA}}(Q, E_1) - f_{EC}\left(\frac{E_0}{Q}\right)\right], \tag{1}$$

where the privacy amplification factor is

$$f_{\text{PA}}(Q, E_1) = \frac{r_{\text{tag}}}{Q} + \left(1 - \frac{r_{\text{tag}}}{Q}\right)\text{h}\left(\frac{E_1}{Q - r_{\text{tag}}}\right), \tag{2}$$

$$r_{\text{tag}} = 1 - \sum_{m=0}^{L/2} e^{-\mu L}\mu^m \frac{(L+1-m)!}{m!(L+1-2m)!}, \tag{3}$$

n_{rep} is the repetition rate of the source laser, p_0 is the probability of Alice preparing a state in the data basis, Q is the total gain, L is the block length, and $E_{0,1}$ are the errors in the data and check basis, respectively. h(x) is the binary entropy function truncated to 1 at x values over 0.5 and the error correction factor $f_{EC}(E_0/Q) = \text{h}(E_0/Q)$.

Due to its small block size, the BB84 protocol can implement phase randomization in a straightforward manner. A gain-switched pulsed laser can ensure perfect phase randomization,[22] while an asymmetric Mach-Zehnder interferometer (MZI) provides the necessary block size.[23] The increased block sizes required by the DQPS protocol effectively prevent the interferometer-based solution because stabilizing a large number of interferometer arms is a formidable task. An alternative approach would be to use a phase modulator for active block-wise phase randomization,[24] which is attractive in theory but problematic in practice. It would require a high-speed source of perfectly random numbers and infinitely precise electrical modulation signals. We note that the DQPS protocol has not yet been demonstrated, despite its conceptual simplicity.

We implement the DQPS protocol with the directly modulated light source[20] shown in Fig. 1. A slave laser emits a gain-switched train of pulses, whilst a master laser controls the phase of the pulses. A small modulation in the master laser applied temporally between adjacent slave laser pulses allows the phase of the pulses to be precisely controlled without affecting their frequency or intensity. This design produces a transmitter that is compact compared to other phase modulation systems and also features a low power consumption and high stability. This transmitter has previously been demonstrated with established QKD protocols.[20,25]

Alice generates a 512-bit pseudo-random pattern and then assigns a basis to each block based on the probability of sending a "check" and "data" block. Knowing the half-wave voltage of the system, modulations are applied in-between pulses in order to encode the desired phase shifts. This output is passed through a polarization controller to align the light with Bob's MZI and then through a 100 GHz filter to remove unwanted noise. She attenuates her signal to the desired mean photon number. The optimal mean photon number is calculated using a simulation based on Eq. (1) for each experimental distance, which is also used to optimize

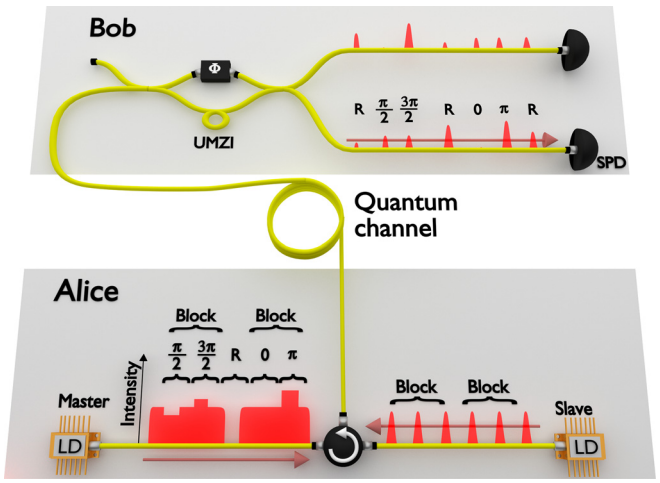

FIG. 1. Experimental setup for the DQPS protocol. A master laser diode (LD) injects phase modulated light into a 2 GHz gain switched slave laser diode via a circulator. We draw $L = 3$ here; however, an arbitrary block size can be set by applying the correct driving signal to the master laser. This is sent to Bob, who interferes the received pulses using an interferometer with a one-bit time-delay and a measurement basis selectable using a phase modulator, Φ, from $\{0, \pi/2\}$, on one arm. Our implementation is proof-of-principle and so uses a thermal phase shifter in one arm. The values he will detect are overlaid on the pulses, with R corresponding to a pulse with a random phase.

the block size. Larger block sizes and a lower mean photon number give better secure key rates at longer distances. The block size is constrained to containing 2^n useful pulses in order to match the pattern size, so $L = 2^n + 1$. She sends the signals to Bob through the quantum channel, which is simulated by an attenuator for some measurements, and using standard optical fiber with a loss of 0.2 dB/km for others.

Bob uses a planar lightwave circuit MZI with a 500 ps time delay on one arm and a heater to select the measurement basis. This component has an inherent 3 dB loss. In our experiment, we use a superconducting nanowire single photon detector (SPD) with a total efficiency of 38.6% and a dark count rate of 15 Hz. The low dark count rate ensures that we are not limited by noise at long distances. The experiment is proof-of-principle, so we measure data in each basis separately, until at least 400 000 counts are detected in both bases. In a real experimental implementation, the basis could be chosen actively for each block, by using a high-speed phase modulator in one arm of the MZI. The output of the SPD is interpreted by a digitizer with 100 ps time bins and a constant fraction discriminator to minimize detection time-jitter. The detectors, laser diodes, and MZI are independently temperature controlled, but no active feedback is given to the system during data collection.

The transmitter in Fig. 1 enables global phase randomization of arbitrarily large block sizes with ease. It does not need an extra phase modulator and a random number generator. The phase continuity of the master laser can be disrupted by driving it below its threshold for a short period of time. A duration of 125 ps is sufficient to deplete the laser cavity field, forcing the subsequent laser pulse to inherit a completely random phase from spontaneous emission. In this regime, the evolution within each block is continuous but is completely random between master emission blocks. Therefore, we are able to achieve both intra-block phase modulation and inter-block phase randomization. After inputting a DQPS pattern, we measure the output intensities from a one-bit interferometer, where all four modulation values are shown alongside the random interference between blocks in Fig. 2. A simulation of the expected inter-block interference intensity shows excellent agreement with the experimental data. We perform an autocorrelation measurement on inter-block interference data and observe that the results are distributed evenly within the expected confidence bounds, further confirming the block randomness. This autocorrelation measurement is shown in Fig. S1 of the supplementary material.

The probability of Bob detecting a "click" in a given time-slot is given by $P^1_{\text{click}} = n/n_{\text{rep}}$, where n is the number of valid detections. From this, we can calculate Q, defined as the probability of having just one click in a block

$$Q = 1 - \left(1 - P^1_{\text{click}}\right)^{L-1}. \tag{4}$$

We use this value alongside the measured QBER and Eqs. 1–3 to calculate our secure key rates.

We now show the resulting secure key rate dependence on channel attenuation (red symbols), Fig. 3(a). Also plotted for comparison are results for the BB84 protocol (black symbols). We can produce secure keys up to a channel

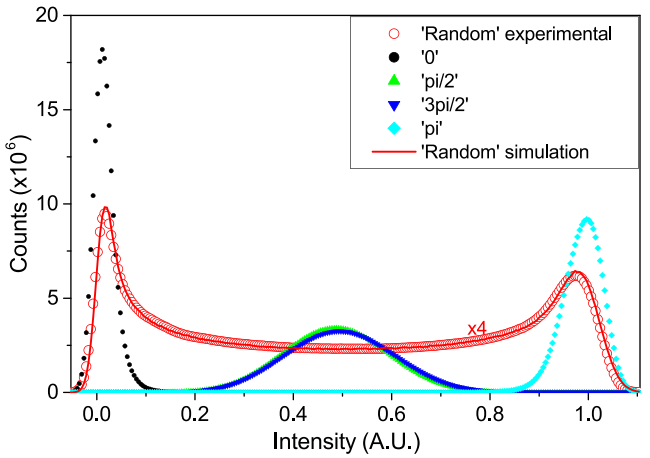

FIG. 2. Randomness of blocks. Histogram of measured intensities for all DQPS signal values after the MZI. Experimental (symbols) data are given and a simulation (line) shows the expected inter-block interference results. The simulation accounts for experimental uncertainties and intensity fluctuations. All of the potential modulation values are plotted and the random signal spans the whole range. The MZI is aligned to measure in the Z basis. 1.95×10^8 samples are taken for each signal value, and the random counts are multiplied by four for visibility.

attenuation of 22 dB, which is equivalent to 110 km of standard optical fiber at 1550 nm, using the DQPS protocol. We also record the data for real fiber lengths of 20, 40, and 60 km, which are well aligned with the simulated results and other experimental data. The secure key rate for DQPS,

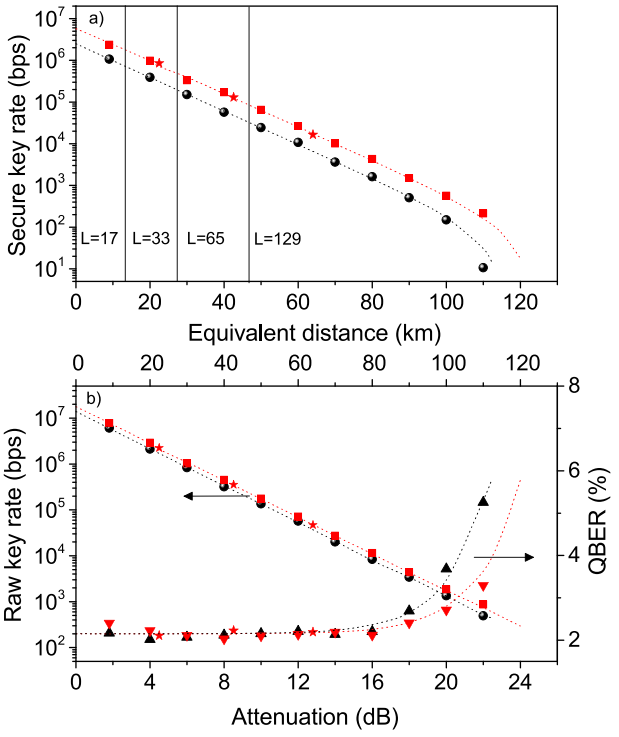

FIG. 3. Protocol results. Experimental (symbols) and simulated (dotted lines) key rates and error rates for optical attenuators and real optical fiber (stars) as the quantum channel. Equivalent distances are calculated assuming standard optical fibre with a loss of 0.2 dB/km at 1550 nm. (a) The secure key rates are shown for DQPS (above, red squares) and BB84 (below, black circles). The block sizes used at each distance for DQPS are overlaid. (b) The raw key rates for DQPS (above, red squares) and BB84 (below, black circles). The QBERs are also displayed for DQPS (red downwards triangles) and BB84 (black triangles).

which reaches megabit per second rates, is higher than BB84 for all channel attenuations, and the DQPS protocol is able to produce secure keys at longer distances. The base QBER is low, at an average of 2.15%. The QBER rises for large attenuations due to the increasing influence of detector dark counts, limiting the secure key rate.

The stability of the free-running system with no active feedback is shown in Fig. 4. The average QBER is $2.03 \pm 0.06\%$, enabling an average secure key rate of 171.272 ± 2.645 kbps, with no drops in secure key over the entire period of 72 h continuous operation. This would amount to a total of 4.95 Gbits of secure key material to be distributed between Alice and Bob.

Phase encoded BB84 is currently a widely used protocol because of its straightforward implementation. We have shown that the DQPS protocol is able to extend the obtainable BB84 key rates by a factor of 2.71 with no consequences on the experimental complexity. As with BB84, the DQPS protocol also offers unconditional security. We note that the performance of the BB84 protocol has been significantly enhanced using decoy states,[26,27] at the expense of implementation simplicity because intensity modulators are required. However, we believe that the decoy-state technique can equally enhance the performance of the DQPS protocol, given that the BB84 protocol is just a special case of the DQPS protocol ($L = 2$).

The promising properties of the transmitter are also highlighted by the experimental results. The base QBER of 2.15% is lower than many other QKD implementations[28,29] and allows us to achieve excellent key rates. A simple change in input patterns to the master and slave lasers allows the transmitter to implement both phase and intensity modulated QKD protocols. This paves the way for single systems that can choose a protocol based on particular clients and also easily adapt to new protocols. Additionally, many current QKD transmitters require time consuming active feedback mechanisms to ensure that the system remains stable;[30] however, the stability data presented in Fig. 4 show that this is unnecessary in the current implementation, giving accurate phase modulation over three days. This could not only lead to greatly simplified practical QKD systems but also increase the key rates because stabilisation pulses are no longer necessary. The secure key rates of the DQPS protocol over three real-fiber distances also align well with the theoretical values and those obtained using an optical attenuator, proving the system's performance in a realistic scenario.

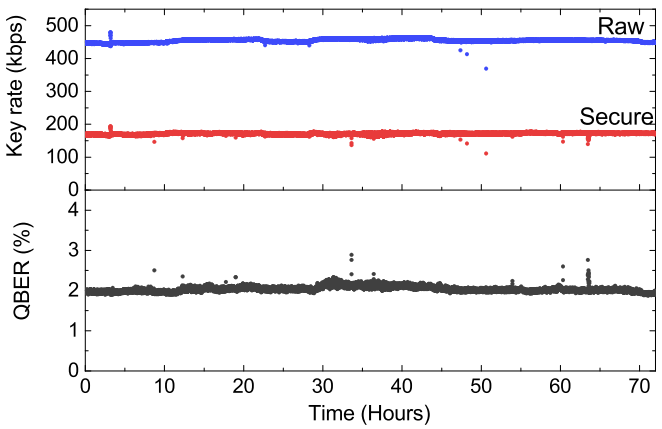

FIG. 4. Stability. The extrapolated key rates are shown alongside the QBER for three days of uninterrupted transmission at 8 dB channel attenuation. $L = 65$, the mean photon number is 0.00722 photons per pulse and the integration time is 4 s. Counts and QBER are measured in the Y basis, and we assume that these are the same in the X basis.

In summary, we have given an experimental demonstration of the DQPS protocol, made possible due to a directly phase modulated quantum transmitter. We have achieved secure key rates almost three times higher than the commonly adopted BB84 protocol and have also shown the excellent stability of the source over three days, removing the need for a QKD system to have complicated active feedback mechanisms. These results provide a foundation for developments in both the transmitter and the protocol that could enhance future quantum communications.

See supplementary material for the autocorrelation results of a DQPS pattern over 100 lags.

G.L.R gratefully acknowledges financial support from the EPSRC CDT in Integrated Photonic and Electronic Systems and Toshiba Research Europe Limited. This work has been supported by funding through the EPSRC Quantum Communications Hub EP/M013472/1.

[1]C. H. Bennett and G. Brassard, in *International Conference on Computer System and Signal Processing*, IEEE (1984), pp. 175–179.
[2]N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3]V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[4]M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Opt. Express **19**, 10387 (2011).
[5]M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, New J. Phys. **11**, 075001 (2009).
[6]G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Phys. Rev. Lett. **115**, 040502 (2015).
[7]K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[8]H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).
[9]D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[10]B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).
[11]D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, Sci. Rep. **6**, 36756 (2016).
[12]T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **109**, 260501 (2012).
[13]A. Mizutani, T. Sasaki, G. Kato, Y. Takeuchi, and K. Tamaki, Quantum Sci. Technol. **3**, 014003 (2018).

[14]S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photonics **9**, 832 (2015).
[15]H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photonics **9**, 827 (2015).
[16]J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **114**, 180502 (2015).
[17]L. Liu, F.-Z. Guo, S.-J. Qin, and Q.-Y. Wen, Sci. Rep. **7**, 42261 (2017).
[18]K. Inoue and Y. Iwai, Phys. Rev. A **79**, 022319 (2009).
[19]S. Kawakami, T. Sasaki, and M. Koashi, Phys. Rev. A **94**, 022322 (2016).
[20]Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, Phys. Rev. X **6**, 031044 (2016).
[21]M. Koashi, New J. Phys. **11**, 045018 (2009).
[22]Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, Appl. Phys. Lett. **104**, 261112 (2014).
[23]A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, Opt. Express **23**, 7583 (2015).
[24]Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).
[25]G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, Laser Photonics Rev. **11**, 1700067 (2017).
[26]H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[27]X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[28]A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).
[29]M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **21**, 24550 (2013).
[30]Z. L. Yuan and A. J. Shields, Opt. Express **13**, 660 (2005).